DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG

22 March 2007

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy # 1: Firewalls

1. References:

   a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

   b. AR 25-2, Information Assurance, 14 November 2003.

   c. DoD Directive 8500.1, "Information Assurance (IA)", 24 October 2002.

   d. DOD Instruction 8500.2, "Information Assurance (IA) Implementation", 6 February 2003.

   e. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation (C&A) Process," 30 December 1997

   f. DoD CIO Guidance and Policy Memorandum (G& PM) No. 8-8001 - "Global Information Grid (GIG)," 31 March 2000

   g. DoD CIO Guidance and Policy Memorandum No 6-8510, "Department of Defense GIG Information Assurance and Information Assurance Implementation Guide", 16 June 2000

   h. 4ID Policy # 5: Passwords, 22 March 2007.

2. Purpose of Policy. Firewalls are primary devices used by the 4ID G6 to safeguard Information Technology (IT) systems and communications resources. Firewalls safeguard IT and data communications resources by restricting access to only those users and connection attempts that comply with pre-defined authorization rule sets and denying access to all other connection attempts.

3. Applicability. This policy applies to, and is an IT / IA operational directive to, all soldiers, civilians, and contractors who plan, deploy, configure, operate, or maintain data communications resources, IA systems, or firewall devices directly or indirectly attached to 4ID networks.

4. Responsibilities.

   a. Chief Information Officer (CIO/G6) will:

      (1) Ensure that appropriate firewall security policies are established.

      (2) Prepare budget and funding requests to support the firewall and other Command and Control Protect (C2P) requirements.

      (3) Implement, operate and document firewall solutions required by 4ID organizations.

   b. Information Assurance Manager (IAM) will:

      (1) Ensure the firewall policy is written that describes the intended functionality of the firewall and that the firewall as installed enforces that policy.

(2) Ensure the policy identifies network assets, allowed services, network choke points, and threats.

(3) Ensure the firewall administrator (SA) receives training to operate the firewall.

c. Information Assurance Security Officer (IASO) will:

(1) Ensure the firewall is certified and accredited in accordance with the DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP), reference 1f.

(2) Ensure that the firewall is operated and maintained according to the vendor's specifications and organizational requirements.

(3) Working with the firewall administrator, ensure that the firewall audit log is reviewed frequently.

(4) Report any security incidents involving the firewall as required by the organizational security regulations, and to the IAPM.

(5) Ensure the firewall security policy is implemented and carried out properly.

(6) Continuously evaluate the firewall security environment. Make recommendations to the IAPM as appropriate.

d. Firewall Administrator will:

(1) Understand and monitor the configuration of the firewall.

(2) Each firewall shall be configured with user ID and password access controls that are compliant with the 4ID password policy.

(3) Ensure that the firewall is continuously afforded effective physical security.

(4) Make frequent backups of data and files on the firewall and ensure that firewall software integrity is maintained. Store configuration backups off line.

(5) Respond to any alarms or alerts from the firewall software as quickly as possible.

(6) In coordination with the IASO, ensure adequate security is maintained over the firewall.

(7) Install IAVA patches and corrective patches to the firewall software as required.

(8) Review the audit logs on the firewall on a daily basis.

(9) Report any attacks or incidents on the firewall to the firewall IASO.

(10) Evaluate each new release of the firewall software to determine if an upgrade is required.

5. Firewall Policy: Centrally managed, consistent firewall solutions will be used throughout 4ID Networks as a primary strategy for safeguarding AIS from unauthorized penetration, access, misuse, or denial of service. Firewall installation and operation must be coordinated with the appropriate TNOSC and RECRT.

a. Firewall Requirements Analysis and Planning:

(1) Firewall deployment shall be preceded by the documentation of connectivity, Information Assurance (IA) and access restriction requirements. User organization and system owner personnel shall communicate their requirements to the firewall administration team, usually through opening a trouble ticket at the 4ID Helpdesk. Requirements shall

be signed-off and approved by an appropriate user-organization decision authority. Minimum functional requirements and planning subjects include:

(a) Organization size (i.e., number of segments and nodes)

(b) Specific connectivity permissions.

(c) Specific connectivity prohibitions.

(d) Bandwidth requirements.

(e) Protocol and Port requirements

(f) Load balancing, alternate routing, and survivability requirements.

(2) Firewall devices shall be selected, configured, tested, validated, and documented per functional requirements. They shall be sized to support the user-organization's current traffic, providing an allowance for anticipated near-term traffic growth. Only firewalls listed on the Army blanket purchase agreement (BPA) may be used.

(3) Firewall rule sets shall be based on the "deny all" philosophy. That is, all connectivity that is not functionally required and specifically requested by system owners shall be denied.

(4) Configure firewall devices with the following IA safeguards to minimize risks of firewall penetration and access rule over-ride by unauthorized personnel:

(a) Disable all services inherent in the firewall device that are not required to provide firewall functionality. For example, disable any non-firewall service provisioning functionality (e.g., FTP or SMTP) when initializing firewall devices. When available, configure firewall devices for protocol specific content filters.

(b) Deny "Public" access to hosts that do not specifically require "Public" access. Hosts requiring public access shall be configured in a DMZ-like environment to minimize public threats to protected network resources.

(c) When providing firewall services, it is paramount that tenant system administrators, subject matter experts, and IA staff confirm and approve firewall rule sets prior to implementation. This will minimize unexpected traffic denial and the need for fast turnaround rule set modifications.

b. Physical Security:

(1) The firewall hardware shall be located in a controlled environment with unescorted access limited to network and firewall administrators.

(2) Anyone entering the firewall enclosure without unescorted access privileges shall sign a visitor's log before entering and upon leaving the firewall enclosure.

(3) The firewall enclosure shall be equipped with heat, air conditioning, and smoke alarms to ensure a proper operating environment for electronic equipment.

(4) The firewall shall be protected against unauthorized hardware or software modifications.

c. Firewall Administrative Security:

(1) The firewall administrator and the alternate shall be trained in administration, operation, and maintenance of the firewall.

(2) The firewall administrator, IASO, and their alternates shall be designated as ADP-I positions and the individuals filling those positions shall have the appropriate background investigations for those positions as specified in AR 380-67.

(3) The firewall shall be accredited in accordance with the DITSCAP.

(4) Systems that are to be protected by the firewall shall be explicitly identified.

d. Location in the Network:

(1) The firewall must be located and configured so that it can monitor and control all communications between the protected network and the systems on the outside of the firewall.

(2) There shall be no modems or dial-in or dial-out connections on the protected network that do not go through the firewall. As an exception, a dial out only modem may be permitted for notifying security personnel of a security event by pager. The modem must be configured to allow only one single phone number for this purpose.

(3) The firewall must be configured so that it cannot be bypassed or circumvented.

(4) The firewall must be configured to withstand deliberate denial-of-service attacks such as SYN flooding or "ping of death" attacks.

(5) Only the firewall administrator or alternate administrator may modify the firewall software.

(6) The firewall shall be configured to be capable of passing encrypted information.

(7) The firewall may not have any compilers, editors, communications software, user applications, or any other files on the firewall other than those directly related to the functioning of the firewall. An intrusion detection system is permitted as an exception.

(8) The firewall shall report, or log, all violations of this policy.

(9) The threshold for reporting or logging incidents or policy violations shall be configured the lowest reasonable level of incidents.

(10) The audit trail and/or security logs shall be maintained in files accessible only by the firewall administrator, the IASO, or their alternates.

(11) The firewall audit trail, or event logs, shall be reviewed by the firewall administrator, or the IASO, or their alternates on a daily basis.

(12) The firewall audit trail, or event logs, shall be maintained on file (tape backup or CD) for a period of 12 months. (The key here is to make the retention period long enough to be able to analyze any incidents that have occurred in the recent past).

(13) Alarm and alert functions on the firewall and any other perimeter access control devices shall be enabled.

(14) The firewall administrator shall be notified of a security alarm by the fastest means possible so that an immediate response may be made to the alarm.

(15) System integrity checks of the firewall shall be performed on a routine basis.

(16) Application level firewalls shall be configured so that outbound network traffic appears as if the traffic had originated from the firewall, i.e., internal addresses are hidden from the outside networks.

(17) The firewall's system integrity database shall be updated each time the firewall's configuration is modified. System integrity files shall be stored on read-only media or on off-line storage media.

(18) The firewall shall be configured to reject all traffic on its external interfaces that appears to be coming from internal network addresses.

(19) The firewall shall have an uninterruptible power supply (UPS). The UPS should have sufficient capacity to facilitate proper shutdown of a firewall.

(20) The firewall shall have backups of all relevant data and files and backups shall be stored in a different secure location. Backups can be used to restore operations. If backups are near the firewall, they may succumb to the same fate as the firewall.

(21) The firewall shall have a Continuity of Operations Plan (COOP).

e. Protocols and Ports:

(1) Allowable protocols. The following protocols and ports may be allowed to pass through the firewall, or to be handled by proxies. The list of allowable protocols should be considered as "candidates" for passing through the firewall as each site should individually determine what they will allow through. (It is important to note that even though the list below states that it may be permitted, if the protocol is NOT used on a particular site, it should still be blocked.)

(a) Common Management Information Protocol (CMIP) ports 163 and 164. CMIP may be allowed through the firewall. The authentication, access control, and security log features shall be enabled.

(b) Domain Name System (DNS), port 53. DNS may be allowed outbound to access name servers. DNS shall not be allowed inbound, as the firewall should conceal the inside addresses.

(c) Echo (ping) Command, port 7. The firewall may be configured to permit outbound "Echo request" (ping) packages and inbound "Echo response" to pass through the firewall, but disallow incoming "Echo request" packets.

(d) Endpoint Map (epmap), port 135. If RPC is enabled, epmap may be allowed through the firewall. Allow one-way, inside out.

(e) File Transfer Protocol (FTP), ports 20 and 21. FTP should be permitted to pass through the firewall outbound. Inbound FTP traffic should only be allowed through the firewall from specific IP addresses. Allow if the connection or session utilizes VPN technology.

(f) Finger command. The finger command may be permitted to pass through the firewall outbound, but all incoming finger requests shall be blocked.

(g) Gopher, ports 70 and >1023. Gopher may only be used if proxied (SOCKS proxy) at the firewall and shall be configured only for outbound use.

(h) Hypertext Transport Protocol (HTTP), ports 1023 and 80. The HTTP protocol may only be used if a proxy exists on the firewall. With proxy, allow outbound HTTP. Incoming HTTP shall be directed to web servers placed on a DMZ.

(i) Internet Control Message Protocol (ICMP). The firewall shall be configured to drop packets without returning an ICMP error message.

(j) Internet Protocol (IP). The firewall shall be configured to drop all packets arriving on the unprotected side with a source address of a machine on the protected side.

(k) Internet Packet Exchange (IPX), port 213. If used on a site, the IPX protocol may be permitted through the firewall.

(l) International Standards Organization-Transport Layer Service Access Protocol (ISO-TSAP), port 102. The ISO-TSAP protocol may be allowed through the firewall. For outbound packets, the packet's source address shall be changed to the firewall's address.

(m) Multipurpose Internet Mail Extension (MIME). MIME may be permitted through the firewall.

(n) Post Office Protocol 3, port 110. POP3 traffic may be permitted to pass through the firewall, but only to the SMTP server.

(o) Remote Procedure Call (RPC), port 530. RPCs may only be permitted outbound. The firewall shall prohibit all inbound RPCs.

(p) Secure Electronic Transaction (SET), port 257. SET may be permitted to pass through the firewall if specifically required.

(q) Secure Hypertext Transfer Protocol (S-HTTP), port 443. S-HTTP may be permitted through the firewall.

(r) Secure Multipurpose Internet Mail Extension (S-MIME). S-MIME may be permitted through the firewall.

(s) Secure Socket Layer (SSL), port 443. SSL may be permitted through the firewall.

(t) Simple Mail Transfer Protocol (SMTP), port 25. SMTP may be permitted through the firewall, but only to the mail server on the protected side.

(u) Telecommunications Network (TELNET), port 23. TELNET may be permitted to pass outbound through the firewall, but shall be prohibited from coming in through the firewall to the protected side, unless a proxy is used specifically configured to control such access.

(v) Transmission Control Protocol (TCP). TCP may be permitted through the firewall. The firewall shall be configured to prevent "SYN flood" attacks.

(w) User Datagram Protocol (UDP). UDP may be permitted through the firewall, but the firewall shall block all UDP packets inbound with a host address of a machine on the protected side.

(x) Virtual Private Network (VPN). The firewall shall establish VPNs whenever possible.

(y) Whois Command, port 43. The firewall may permit outbound whois traffic, but shall block all inbound use of the whois command.

(z) Network Time Protocol (NTP), port 123. Port 123 may be permitted from and to specific network devices only as required to maintain consistent system clock.

(aa) Open Shortest Path First (OSPF). OSPF traffic may be permitted through the firewall only if network routing devices on the protected network must pass OSPF routing information to routing devices on the unprotected network.

(bb) Routing Information Protocol (RIP), port 520. RIP traffic may be permitted through the firewall only if network routing devices on the protected network must pass RIP routing information to routing devices on the unprotected network.

(cc) Simple Network Management Protocol (SNMP), ports 161 and 162. Ports 161 and 162 may be opened only if network devices need to be monitored from outside the protected network. If opened, only specific IP addresses will be allowed through.

(2) Prohibited Protocols.

(a) Archie, port 1525 and >1023. Port 1525 shall be blocked by the firewall.

(b) Exterior Gateway Protocol (EGP). EGP requests shall not be permitted through the firewall.

(c) Internet Relay Chat (IRC), port 194. Port 194 shall be blocked by the firewall.

(d) Network File System (NFS), port 2049. Port 2049 shall be blocked by the firewall.

(e) Network Information Service (NIS). NIS traffic shall not be permitted through the firewall.

(f) Network News Transfer Protocol (NNTP), port 119. Port 119 shall be blocked by the firewall.

(g) Open Windows, port 2000. Port 2000 shall be blocked by the firewall.

(h) Remote Execution (rexec), port 512. Port 512 shall be blocked by the firewall.

(i) Remote Login (rlogin), port 513. Port 513 shall be blocked by the firewall.

(j) Restricted Shell (rsh), port 514. Port 514 shall be blocked by the firewall.

(k) Remote Access Protocol (RAP), port 38. Port 38 shall be blocked by the firewall.

(l) Trivial File Transfer Protocol (TFTP), port 69. Port 69 shall be blocked by the firewall.

(m) UNIX-to-UNIX Copy (UUCP), port 540. Port 540 shall be blocked by the firewall.

(n) Wide-Area Information Service (WAIS), ports 210 and >1023. Port 210 shall be blocked by the firewall.

(o) X-Windows (X11), port 6000-6063. Port 6000-6063 shall be blocked by the firewall.

f. Initial configurations shall establish configuration management baselines on a user organization and correlated firewall. Required configurations shall be thoroughly tested, validated, and documented before placing new firewalls or configuration modifications into production.

g. Firewall Configuration Management, Testing, Validation, and Documentation: Firewall architecture and capacity planning shall be included in annual Service Level Agreements (SLAs) and Inter-Service Support Agreements (ISSAs).

h. New software releases, configuration updates, and access rule modifications shall be documented, tested, validated, approved by the Configuration Control Board (CCB) and added to configuration management records prior to deployment.

i. Operation and Maintenance:

(1) Firewall Device Access Controls:

(a) Individual administrators and technicians who access, repair, and modify firewall configurations shall be specifically identified.

(b) Individuals accessing firewall devices are required to enter a user ID and password. User profiles shall govern the access rights of the user.

(c) Guest accounts shall be disabled.

(d) Administrator accounts shall be renamed.

(e) Sharing of accounts and passwords will not be permitted.

(f) Password expiration cycles shall be defined and enforced.

(g) The passwords will be remembered for one year and may not be recycled during that time.

(h) Accounts will be locked after 3 unsuccessful attempts within a 30-minute period and the firewall administrator and IASO notified.

(i) Only firewall administrators shall be able to unlock accounts.

(j) Audit records shall be generated to document when account lockouts occur.

(k) The use of shared group ID's will not be allowed. However, the use of Group memberships, where users maintain individual user ID's and the Group membership controls rights and permissions for the group, is permissible.

(l) Remote administration of firewalls over the NIPRNet, Internet, etc., shall be accomplished via secure communications path (e.g., VPN technology, etc.).

(2) Accountability: Audit information shall be retained and protected so that actions affecting security can be traced to the responsible party.

(3) Assurance: Firewall devices shall contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces requirements 5.d to 5.e above.

(4) Continuous Protection:

(a) Data from "trusted" mechanisms that document firewall device system administration, rule set modifications, operation, and performance shall be continuously protected against tampering and/or editing.

(b) Attempts to modify system services, whether successful or not, shall be recorded and retained in security logs.

(c) Security, application, and system audit logs shall be copied nightly. Systems shall be backed up on a regular basis and stored in secure directories. Additional tape backup or CD copies of system files shall be created and readily available for use by IA staff.

(5) Documentation and Configuration Management:

(a) Maintenance of up-to-date firewall configuration documentation and configuration management records is the responsibility of the firewall administrators.

(b) Changes to the configuration baseline shall be in accordance with the Configuration Management Plan (CMP) and coordinated and/or approved by the Configuration Control Board (CCB).

6. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding